CLAIMS

What is claimed is:

1. A card device for communication with an electronic device, comprising:

a memory for storing a capabilities list associated with an application program, said capabilities list including information regarding access to one or more resources for use by said application program, and for storing said application program and a security manager; and

a processing unit for executing said application program and said security manager, said security manager for selectively granting access to said one or more resources for use by said application program based at least in part on said capabilities list.

2. The card device of claim 1 wherein said one or more resources comprise at least one of data and functions.

3. The card device of claim 1 wherein said one or more resources comprise one or more resources external to said card device.

4. The card device of claim 3, further comprising at least one of:

terminal side resources; and

channels of a communications network.

5. The card device of claim 1 wherein said one or more resources comprise one or more resources owned by at least one of said application program and another entity.

6. The card device of claim 5 wherein said other entity comprise at least one of:

an operating system of said card device; and

another application program.

7. The card device of claim 1 wherein said capabilities list comprises information regarding at least one of:

access rights; and

information required for access to a resource.

8. The card device of claim 1 wherein said memory stores a first capabilities list and a second capabilities list, said first capabilities list comprising a handle to link to said second capabilities list.

9. The card device of claim 8 wherein said second capabilities list is associated with one or more of other application programs.

10. The card device of claim 1 wherein said application program is for requesting access to a resource.

11. The card device of claim 1 wherein

said application program is for transmitting a resource access request to a security manager; and

said security manager is for transmitting a verify request to a verification program to examine said capabilities list to determine whether said application program is authorized to access said resource, and for performing or denying said requested action based at least in part on said examination.

12. The card device of claim 11 wherein said security manager comprises an application program interface (API).

13. The card device of claim 11 wherein said security manager is for obtaining information regarding said requesting application program through one of inquiring at a context originating the resource access request and a parameter provided with said resource access request.

14. The card device of claim 1, further comprising input/output means for receiving said capabilities list from at least one of a provider of said application program and an owner of said one or more resources.

15. The card device of claim 1 wherein said capabilities list and said application program constitute a load package received by said card device.

16. The card device of claim 1 wherein said device is configured to modify said capabilities list based at least in part on a subsequently received capabilities update list associated with said application program.

17. The card device of claim 1 wherein said device is configured to delete said capabilities list or link and access rights upon receiving an instruction to delete said application program from the outside.

18. The card device of claim 1 wherein

said capabilities list is encrypted; and

said processor is configured to decrypt said capabilities list.

19. The card device of claim 1 wherein

said capabilities list is cryptographically signed by at least one of a provider of said application program and an owner of said one or more resources; and

said processor is configured to cryptographically authenticate said capabilities list.

20. The card device of claim 19 wherein said processor is further configured to cryptographically authenticate said capabilities list when said capabilities list is stored on said device.

21. The card device of claim 19 wherein said processor is further configured to cryptographically authenticate said capabilities list when said capabilities list is accessed,

said capabilities list being successfully authenticated if a first fingerprint computed over said capabilities list upon storing capabilities list matches a second fingerprint computed over said capabilities list in response to a run-time request to use said capabilities list.

22. The card device of claim 1 wherein said application program comprises a plurality of modules.

23. The card device of claim 1 wherein said application program comprises a Java application program or a Java Card™ applet.

24. The card device of claim 1 wherein said capabilities list is embodied in a tag-length-value (TLV) structure.

25. A method for controlling a card device, the card device for communication with an electronic device, the method comprising:

storing an application program on said card device;

storing a capabilities list associated with said application program on said card device, said capabilities list comprising information regarding access to one or more resources for use by said application program; and

executing said application program and a security manager, said security manager for selectively granting access to said one or more resources for use by said application program based at least in part on said capabilities list.

26. The method of claim 25 wherein said one or more resources comprise at least one of data and functions.

27. The method of claim 25 wherein said one or more resources comprise one or more resources external to said card device.

28. The method of claim 27 wherein said card device further comprises at least one of:
terminal side resources; and
channels of a communications network.

29. The method of claim 25 wherein said one or more resources comprise one or more resources owned by at least one of said application program and another entity.

30. The method of claim 29 wherein said other entity comprises at least one of:
an operating system of said card device; and
another application program.

31. The method of claim 25 wherein said capabilities list comprises information regarding at least one of:
access rights; and
information required for access to a resource.

32. The method of claim 25 wherein said information included in said memory stores a first capabilities list and a second capabilities list, said first capabilities list comprising a handle to link to said second capabilities list.

33. The card device of claim 32 wherein said second capabilities list is associated with one or more of other application programs.

34. The method of claim 25 wherein said executing further comprises said application program requesting access to a resource.

35. The method of claim 25 wherein said executing further comprises:

said application program transmitting a resource access request to said security manager; and

said security manager transmitting a verify request to a verification program to examine said capabilities list to determine whether said application program is authorized to access said resource, and performing or denying the requested action based at least in part on said examination.

36. The method of claim 35 wherein said security manager comprises an application program interface (API).

37. The method of claim 35 wherein said security manager obtains information regarding said requesting application program through and least one of inquiring at a context originating said resource access request, and a parameter provided with said resource access request.

38. The method of claim 25, further comprising receiving said capabilities list from at least one of a provider of said application program and an owner of said one or more resources.

39. The method of claim 25 wherein said capabilities list and said application program are comprised in a load package received by said card device.

40. The method of claim 25, further comprising modifying said capabilities list based at least in part on a subsequently received capabilities update list associated with said application program.

41. The method of claim 25, further comprising deleting said capabilities list or link and access rights upon receiving an instruction to delete said application program from the outside.

42. The method of claim 25 wherein

said capabilities list is encrypted; and

said method further comprises decrypting said capabilities list.

43. The method of claim 25 wherein

said capabilities list is cryptographically signed by at least one of a provider of said application program and an owner of said one or more resources; and

said method further comprises cryptographically authenticating said capabilities list.

44. The method of claim 25, further comprising cryptographically authenticating said capabilities list when said capabilities list is stored on said device.

45. The method of claim 25, further comprising cryptographically authenticating said capabilities list when said capabilities list is accessed, said capabilities list being successfully authenticated if a first fingerprint computed over said capabilities list upon storing capabilities list matches a second fingerprint computed over said capabilities list in response to a run-time request to use said capabilities list.

46. The method of claim 25 wherein said application program comprises a plurality of modules

47. The method of claim 25 wherein said application program comprises a Java application program or a Java Card™ applet.

48. The method of claim 25 wherein said capabilities list is embodied in a tag-length-value (TLV) structure.

49. A program storage device readable by a machine, embodying a program of instructions executable by the machine to perform a method for controlling a card device, the card device for communication with an electronic device, the method comprising:

storing an application program on said card device;

storing a capabilities list associated with said application program on said card device, said capabilities list comprising information regarding access to one or more resources for use by said application program; and

executing said application program and a security manager, said security manager for selectively granting access to said one or more resources for use by said application program based at least in part on said capabilities list.

50. The program storage device of claim 49 wherein said one or more resources comprise at least one of data and functions.

51. The program storage device of claim 49 wherein said one or more resources comprise one or more resources external to said card device.

52. The program storage device of claim 51 wherein said card device further comprises at least one of:

terminal side resources; and

channels of a communications network.

53. The program storage device of claim 49 wherein said one or more resources comprise one or more resources owned by at least one of said application program and another entity.

54. The program storage device of claim 53 wherein said other entity comprises at least one of:
an operating system of said card device; and
another application program.

55. The program storage device of claim 49 wherein said capabilities list comprises information regarding at least one of:
access rights; and
information required for access to a resource.

56. The program storage device of claim 49 wherein said information included in said memory stores a first capabilities list and a second capabilities list, said first capabilities list comprising a handle to link to said second capabilities list.

57. The program storage device of claim 56 wherein said second capabilities list is associated with one or more of other application programs.

58. The program storage device of claim 49 wherein said executing further comprises said application program requesting access to a resource; and

59. The program storage device of claim 49 wherein said executing further comprises:

said application program transmitting a resource access request to said security manager; and

said security manager transmitting a verify request to a verification program to examine said capabilities list to determine whether said application program is authorized to access said resource, and performing or denying the requested action based at least in part on said examination.

60. The program storage device of claim 59 wherein said security manager comprises an application program interface (API).

61. The program storage device of claim 59 wherein said security manager obtains information regarding said requesting application program through and least one of inquiring at a context originating said resource access request, and a parameter provided with said resource access request.

62. The program storage device of claim 49, said method further comprising receiving said capabilities list from at least one of a provider of said application program and an owner of said one or more resources.

63. The program storage device of claim 49 wherein said capabilities list and said application program are comprised in a load package received by said card device.

64. The program storage device of claim 49, said method further comprising modifying said capabilities list based at least in part on a subsequently received capabilities update list associated with said application program.

65. The program storage device of claim 49, said method further comprising deleting said capabilities list or link and access rights upon receiving an instruction to delete said application program from the outside.

66. The program storage device of claim 49 wherein

said capabilities list is encrypted; and

said method further comprises decrypting said capabilities list.

67. The program storage device of claim 49 wherein

said capabilities list is cryptographically signed by at least one of a provider of said application program and an owner of said one or more resources; and

said method further comprises cryptographically authenticating said capabilities list.

68. The program storage device of claim 67, said method further comprising cryptographically authenticating said capabilities list when said capabilities list is stored on said device.

69. The program storage device of claim 67, said method further comprising cryptographically authenticating said capabilities list when said capabilities list is accessed, said capabilities list being successfully authenticated if a first fingerprint computed over said capabilities list

upon storing capabilities list matches a second fingerprint computed over said capabilities list in response to a run-time request to use said capabilities list.

70. The program storage device of claim 49 wherein said application program comprises a plurality of modules.

71. The program storage device of claim 49 wherein said application program comprises a Java application program or a Java Card™ applet.

72. The program storage device of claim 49 wherein said capabilities list is embodied in a tag-length-value (TLV) structure.

73. An apparatus for controlling a card device, the card device for communication with an electronic device, the apparatus comprising:

means for storing an application program on said card device;

means for storing a capabilities list associated with said application program on said card device, said capabilities list comprising information regarding access to one or more resources for use by said application program; and

means for executing said application program and a security manager, said security manager for selectively granting access to said one or more resources for use by said application program based at least in part on said capabilities list.

74. The apparatus of claim 73 wherein said one or more resources comprise at least one of data and functions.

75. The apparatus of claim 73 wherein said one or more resources comprise one or more resources external to said card device.

76. The apparatus of claim 75 wherein said card device further comprises at least one of:
terminal side resources; and
channels of a communications network.

77. The apparatus of claim 73 wherein said one or more resources comprise one or more resources owned by at least one of said application program and another entity.

78. The apparatus of claim 77 wherein said other entity comprises at least one of:
an operating system of said card device; and
another application program.

79. The apparatus of claim 73 wherein said capabilities list comprises information regarding at least one of:
access rights; and
information required for access to a resource.

80. The apparatus of claim 73 wherein said information included in said memory stores a first capabilities list and a second capabilities list, said first capabilities list comprising a handle to link to said second capabilities list.

81. The card device of claim 80 wherein said second capabilities list is associated with one or more of other application programs.

82. The apparatus of claim 73 wherein said means for executing further comprises said means for requesting access to a resource.

83. The apparatus of claim 73 wherein said means for executing further comprises:

said application program transmitting a resource access request to said security manager; and

said security manager transmitting a verify request to a verification program to examine said capabilities list to determine whether said application program is authorized to access said resource, and performing or denying the requested action based at least in part on said examination.

84. The apparatus of claim 73 wherein said security manager comprises an application program interface (API).

85. The apparatus of claim 73 wherein said security manager obtains information regarding said requesting application program through at least one of inquiring at a context originating said resource access request, and a parameter provided with said resource access request.

86. The apparatus of claim 73, further comprising means for receiving said capabilities list from at least one of a provider of said application program and an owner of said one or more resources.

87. The apparatus of claim 73 wherein said capabilities list and said application program are comprised by in a load package received by said card device.

88. The apparatus of claim 73, further comprising means for modifying said capabilities list based at least in part on a subsequently received capabilities update list associated with said application program.

89. The apparatus of claim 73, further comprising means for deleting said capabilities list or link and access rights upon receiving an instruction to delete said application program from the outside.

90. The apparatus of claim 73 wherein

said capabilities list is encrypted; and

said method further comprises decrypting said capabilities list.

91. The apparatus of claim 73 wherein

said capabilities list is cryptographically signed by at least one of a provider of said application program and an owner of said one or more resources; and

said method further comprises cryptographically authenticating said capabilities list.

92. The apparatus of claim 91, further comprising means for cryptographically authenticating said capabilities list when said capabilities list is stored on said device.

93. The apparatus of claim 91, further comprising means for cryptographically authenticating said capabilities list when said capabilities list is accessed, said capabilities list being successfully authenticated if a first fingerprint computed over said capabilities list upon storing capabilities list matches a second fingerprint computed over said capabilities list in response to a run-time request to use said capabilities list.

94. The apparatus of claim 73 wherein said application program comprises a plurality of modules

95. The apparatus of claim 73 wherein said application program comprises a Java application program or a Java Card™ applet.

96. The apparatus of claim 73 wherein said capabilities list is embodied in a tag-length-value (TLV) structure.

97. A memory for storing data for access by an application program being executed on a data processing system, comprising:

a data structure stored in said memory, said data structure including information used by said application program to determine at run-time information regarding access to one or more resources for use by said application program.

98. The memory of claim 97 wherein said memory is for storing said application program and said data structure.

99. The memory of claim 98 wherein said application program and said data structure are contiguous in said memory.

100. The memory of claim 98 wherein said data structure is stored within said application program in said memory.